Honorable John C. Coughenour

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

ZANGO, INC., Plaintiff, v. KASPERSKY LAB, INC., Defendant.	No. C-07-0807-JCC DECLARATION OF SHANE COURSEN IN SUPPORT OF OPPOSITION TO PLAINTIFF'S MOTION FOR TEMPORARY RESTRAINING ORDER

I, Shane Coursen, declare as follows:

1. I am the Senior Technical Consultant for Kaspersky Lab, Inc.("Kaspersky USA"). I have been employed by Kaspersky USA for just over two years, since January or February of 2005. I have personal knowledge of the facts discussed below.

2. Kaspersky USA resells internet security software developed in Moscow by a Russian company, Kaspersky Lab ZAO ("Kaspersky Moscow"). Internet security software includes anti-virus software, spam (*i.e.*, junk e-mail) filters, firewalls (software that regulates communication between computer networks), and related software and databases. As such, Kaspersky provides a valuable product for computer users. Specifically, the Kaspersky software products help guard computers from "malware." "Malware" is short for "malicious software" and is the umbrella term for a host of unwanted software programs that can invade

Davis Wright Tremaine LLP
LAW OFFICES
2600 Century Square · 1501 Fourth Avenue
Seattle, Washington 98101-1688
(206) 622-3150 · Fax: (206) 628-7699

privacy, delete or damage computer files, steal identities, open unwanted links to pornography websites (thus potentially exposing children to obscene materials), and otherwise hinder operation of individual computers or entire computer networks. Contemporary malware spreads from computer to computer over the Internet, such as by e-mail. Computer users may also expose their computers to malware when they download videos, games, software programs, or other content from malicious websites. Malware is hard to discover. Furthermore, once discovered, it is hard to remove from the computer. For the reasons discussed below, I believe that Zango exposes computer users to malware.

3. Malware includes, for example, computer viruses, worms, spyware, and potentially unwanted software, such as adware. Each of these terms is defined below:

a. Virus. A computer virus is an unwanted software program that, like a biological virus, infects a host computer, replicates itself, and then spreads to other computers. Like biological viruses, viruses can lie dormant, cause no damage, or, more typically, cause substantial damage to a host computer. For example, computer viruses can automatically delete or corrupt computer files. Other viruses can open a "backdoor" into somebody's computer, allowing a computer hacker or cyber thief to gain access to a computer user's personal files, thus stealing the user's identity or, perhaps, vandalizing the user's computer files.

b. Worm. A computer worm is like a virus but spreads from computer to computer in a different way. Worms can also cause substantial damage to computers or computer networks.

c. Spyware. Spyware is an unwanted computer program that gains access to and resides on a computer without the user's knowledge. Spyware collects information about a computer user's activities and covertly sends that information to a computer hacker or other unscrupulous person. For example, some spyware monitors a computer user's Internet browsing habits and reports which websites the user visits.

Davis Wright Tremaine LLP
LAW OFFICES
2600 Century Square · 1501 Fourth Avenue
Seattle, Washington 98101-1688
(206) 622-3150 · Fax: (206) 628-7699

Spyware can also monitor a computer user's keystrokes. A computer hacker can thus use spyware to discover a user's passwords, social security number, and other personal, confidential information. Spyware, once detected, is often very difficult to uninstall and remove from a computer.

d. Adware. Adware can be like spyware, but a computer user sometimes knowingly downloads it, with consent, onto his or her computer system. Adware can also reduce the effectiveness of a computer's security systems, without the user's knowledge or consent. Adware typically monitors a computer user's Internet browsing habits and causes ads (pop-up ads or banner ads) to appear on the computer user's screen based on the user's browsing habits. For example, a computer user who regularly visits websites devoted to a hobby like gardening may be presented with pop-up ads from seed companies, garden stores, gardening books, and the like. While in theory that is the way adware should work, in practice, the ads displayed on a user's screen may be random and have no correlation with the user's interests. For example, as discussed below, adware can often cause ads for adult oriented content websites (pornography) to appear. Adware can also open links to websites and computer servers that are known to expose computers to viruses and other malware. One particular problem with adware (and, indeed, other malware) is that it can use up computer memory and processing speed and thus slow the operation of a computer.

4. As Senior Technical Consultant, I conduct research on, analyze, and monitor the Internet for malware and try to find ways to combat such malware. I also report to the public and interact with the media on the status of computer viruses and other malware and attempts to defeat them. That is, I issue advisories on computer security threats, like new viruses or worms. In effect, I am a security consultant, charged with tracking, combating, and reporting on malware. Another way to describe my job is that I am like an epidemiologist at

Davis Wright Tremaine LLP
LAW OFFICES
2600 Century Square · 1501 Fourth Avenue
Seattle, Washington 98101-1688
(206) 622-3150 · Fax: (206) 628-7699

the Centers for Disease Control. That is, I track the spread of computer viruses and other malware, warn the public, and help computer users prevent infection.

5. I also serve as a technical liaison between Kaspersky USA and Kaspersky Moscow. Thus, I report problems with the software to Kaspersky Moscow or, for example, alert Moscow to new computer virus outbreaks. I do not, however, have any say in or control over how Kaspersky Moscow handles a problem once reported. Nor do I have any involvement in the design, development, or writing of the Kaspersky software.

6. One way to prevent infection from malware is to install security software like the Kaspersky Internet Security ("KIS") or Kaspersky Anti-Virus ("KAV") systems. The KIS and KAV systems detects adware, spyware, viruses, and other malware and warns the user about it. The KIS and KAV systems then allow the computer user to block or uninstall the malware. For example, a user visits an Internet web site and downloads a video or other software program. Hidden in the download could be a virus, spyware, or other form of malware. The KIS and KAV systems provides a warning message and then gives the user the option of accepting or rejecting the downloaded program.

7. This Kaspersky security software is programmed to be smart and selective. That is, the software does not indiscriminately block all websites and software downloads. Indeed, it allows access to trusted websites and downloads from trusted sources. By "trusted," I mean websites and sources of software that have proven to be free of malware infections. The Kaspersky anti-virus software, however, allows a user to block a website that is known to host malware, pornography, and other unwanted content.

8. The Kaspersky security software does not actually touch, deface, or otherwise have any contact with the untrustworthy websites it detects. Zango claims in its motion papers that the Kaspersky software has somehow defaced or damaged its websites. But that could never be so. All the Kaspersky software does is to detect untrustworthy websites and blocks content from being downloaded onto an unsuspecting user's computer.

Davis Wright Tremaine LLP
LAW OFFICES
2600 Century Square · 1501 Fourth Avenue
Seattle, Washington 98101-1688
(206) 622-3150 · Fax: (206) 628-7699

9. I am familiar with Zango and its affiliated websites (www.zango.com and www.seekmo.com). Zango, formerly known as 180 Solutions, has an unsavory reputation in the Internet security industry. Long before this lawsuit began, I had researched Zango and followed its exploits. Based on my research and my knowledge of the industry, Zango has been a source of malware for several years. Zango's business model is as follows. Zango sponsors websites that allow end users to download, for free, videos (like YouTube videos), computer games, and other computer programs. The free videos are simply a lure for the adware or spyware. The hidden cost of the free downloads is that the user also simultaneously downloads adware or spyware. In turn, the adware displays ads on an end user's computer by linking the end user to the computer servers of various websites. Presumably, the advertisers pay Zango for each time a pop-up or banner ad is displayed on an end user's computer screen via the adware.

10. For sure, some of the websites to which the Zango adware provides links are perfectly trustworthy and harmless. The problem, however, is that the adware often links users to blacklisted, untrustworthy websites containing pornography and malware.

11. For some time, end users who downloaded videos or other programs from Zango websites did not know that they were also downloading the Zango adware. Once adware is installed on a system, it is often hard to remove and clogs computer memory and processing time. Complaints started to be filed. Eventually, the Federal Trade Commission ("FTC") took action against Zango and reprimanded it for what the FTC labeled as deceptive conduct. Attached as Exhibit A is the FTC's order, which resulted from a consent agreement with Zango. The order provides that Zango must pay the FTC $3,000,000 to settle the claims against it. Zango also promised that it would not inject its adware into end users systems without their informed consent.

12. The FTC order went into effect on March 7, 2007. According to Greg Berretta's declaration, Zango allegedly discovered on March 8, 2007--the very next day--that

Davis Wright Tremaine LLP
LAW OFFICES
2600 Century Square · 1501 Fourth Avenue
Seattle, Washington 98101-1688
(206) 622-3150 · Fax: (206) 628-7699

the KIS software was damaging a Zango website, www.seekmo.com. The timing cannot be a coincidence. To me, Zango fabricated a dispute with Kaspersky and other security software providers as a way to extort money to help it pay the FTC settlement or to create the false impression that Zango is somehow a victim. Far from it, Zango is a purveyor of malware.

13. Internet security analysts, experts, and others have kept track of Zango and its operations and have universally criticized Zango. I have collected various blogs (*i.e.*, web logs) and articles about Zango's activities. Attached as Exhibit B are sample blogs and articles, including (1), a Wikipedia entry on Zango reporting various criticisms of Zango's adware and spyware, (2) an article by Ben Edelman and Eric Howes criticizing Zango for failing to comply with terms of the FTC consent order, (3) a news bulletin entitled "Zango Still in Spyware Game," and (4) a blog entitled, "Zango Affiliate Admits to Targeting Kids; What Will Zango Do?" This last blog reports on the activities of Chris Boyd, a noted Internet security researcher who has tracked and uncovered Zango's questionable practices.

14. Currently, the Zango website www.zango.com works as follows. A user clicks on a video or game that he or she wishes to download and selects "Play." The following message then appears:

> Thanks to Zango, the premium content on this website is free, paid for by advertising. When installed, Zango software presents ads (based on keywords from your Internet browsing) in the Zango Toolbar and in a separate browser window that pops up on your screen. Zango is always running and will upgrade automatically. You can uninstall Zango via Add/Remove Programs, but then won't have access to most Zango content.

This message, however, is not displayed prominently. I have found that users typically do not notice or pay attention to the terms of the download. In other words, even with this notice, the unsuspecting user often does not realize that in downloading the video or game, he or she is also downloading the Zango adware.

15. The Kaspersky software does not actually block the Zango adware itself. Indeed, the Kaspersky software allows the user to install the Zango adware, should the user desire. The problem, however, is that once the Zango adware starts running on a computer, it will start linking to untrustworthy file servers or websites. Then and only then will the

Davis Wright Tremaine LLP
LAW OFFICES
2600 Century Square · 1501 Fourth Avenue
Seattle, Washington 98101-1688
(206) 622-3150 · Fax: (206) 628-7699

Kaspersky software provide a warning and allow the user to block the download of content (including ads and, more importantly, viruses, spyware, and other malware) from those sources. These sources often advertise or provide links to pornography websites.

16. I must stress that the Kaspersky security software does not specifically target or single out Zango. As stated above, the Kaspersky software actually allows a user to install the Zango adware, should the user desire. Nor, to my knowledge, does Kaspersky USA have any intent to harm Zango. Kapersky USA's only motive is to provide its customers with the means to protect their computers from malware and other unwanted content. The software is merely a door lock or alarm system that the computer user can turn on or off.

17. The Kaspersky security software (such as the KIS and KAV systems) has different levels of detection and prevention.

a. For example, the software automatically detects certain particularly harmful malware such as viruses, worms, trojan horses, and backdoors. As I understand it, the mere detection of this malware is a basic function of the software and cannot be disabled.

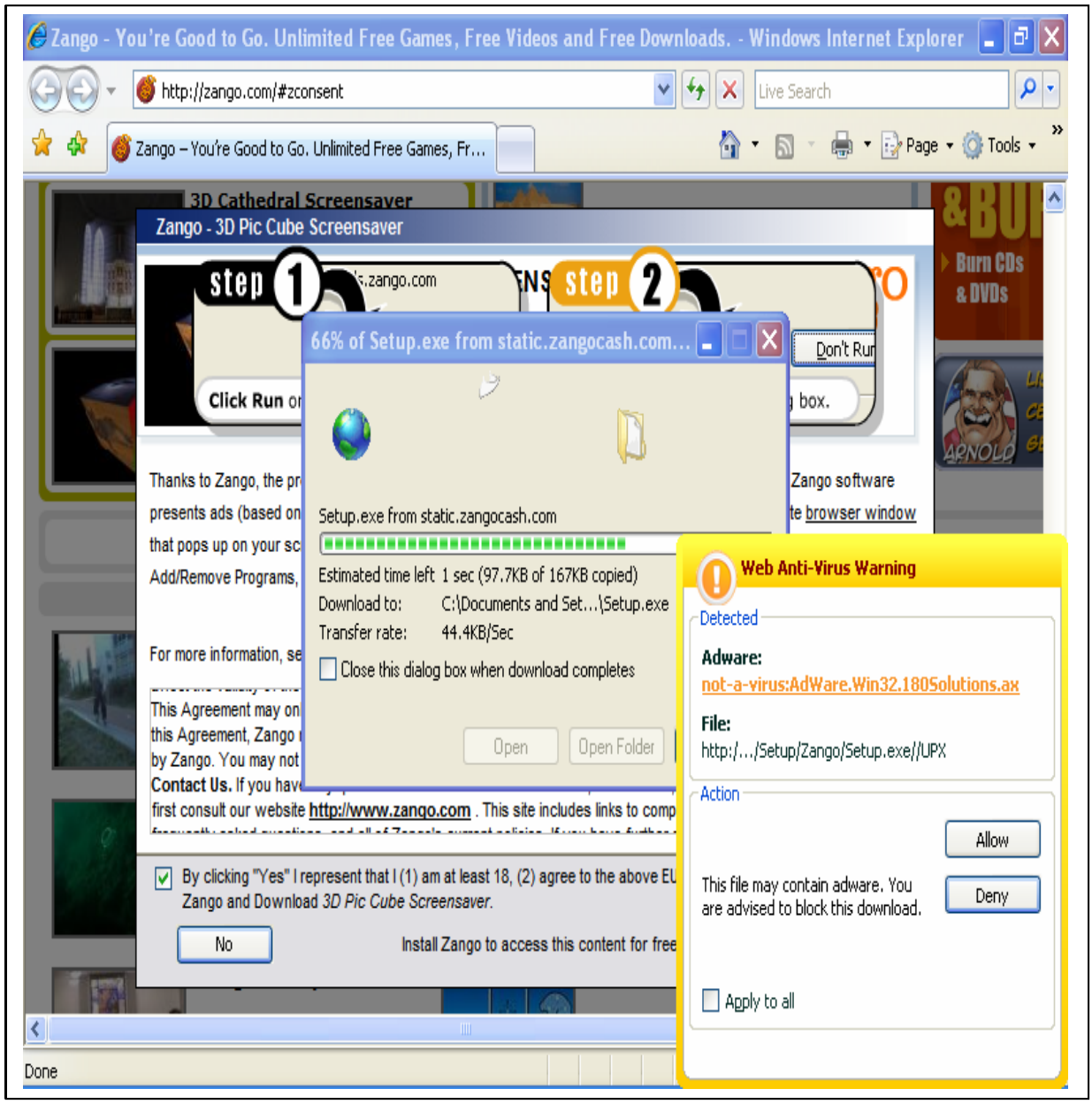
b. The Kaspersky software also detects spyware and adware by default, but users have the option to disable detection of these programs. Accordingly, the Kaspersky security software gives users the choice of accepting the Zango adware. Moreover, the user has the choice whether to block access to certain websites, although the Kaspersky software always blocks malicious websites (*e.g.*, websites that can infect a computer with viruses). In other words, the Kaspersky software allows the user to accept or reject ads from various sources, just as a homeowner can choose to admit a door-to-door salesman or slam the door.

c. Finally, the Kaspersky security software has a feature--which is turned off by default but can be activated--that allows IT professionals to detect and

Davis Wright Tremaine LLP
LAW OFFICES
2600 Century Square · 1501 Fourth Avenue
Seattle, Washington 98101-1688
(206) 622-3150 · Fax: (206) 628-7699

disable certain potentially unwanted software that may be present on a company's or organization's computer network.

18. Shown below is a typical anti-virus warning that the Kaspersky software displays when it detects a potential threat to the user's computer. In this case, the Kaspersky software (running on my computer) has detected adware bundled with a screensaver program that I tried to download from the Zango website. As one can see, the message gives the user the option to "Allow" or "Deny" the download of the adware.



Davis Wright Tremaine LLP
LAW OFFICES
2600 Century Square · 1501 Fourth Avenue
Seattle, Washington 98101-1688
(206) 622-3150 · Fax: (206) 628-7699

19. I have had some communications with Greg Berretta of Zango. Indeed, I passed along to Kaspersky Moscow Greg's request that Kaspersky Moscow remove Zango from its blacklist of untrustworthy Internet sources. As I understand it, Kaspersky Moscow did investigate the matter and did agree to remove certain types of security threat detection. But Kaspersky Moscow did not remove all threat detection. The problem, as stated above, is that while Zango adware does provide links to harmless ads and websites, it just as often provides links to pornography and other untrustworthy sites. It would be highly irresponsible for an Internet security company to remove detection of such sites. Indeed, it would be akin to a CDC epidemiologist knowingly allowing entry into this country of poultry infected with the avian flu.

20. Mr. Berretta claims that Kaspersky admitted that its software has damaged Zango websites. I never admitted any such thing, and I am not aware of anybody from either Kaspersky USA or Kaspersky Moscow admitting as such. It would be physically impossible for the Kaspersky software to damage Zango's website because the software does not touch the website in any way. As stated above, the software merely prevents content from an untrustworthy source (a website or file server) from infecting a computer. The Kaspersky software resides only on the user's computer. It does not inject itself onto the server hosting a website. That is, the software defends a computer but never goes on the offensive to attack a website.

Davis Wright Tremaine LLP
LAW OFFICES
2600 Century Square · 1501 Fourth Avenue
Seattle, Washington 98101-1688
(206) 622-3150 · Fax: (206) 628-7699

PURSUANT TO 28 U.S.C. § 1746, I DECLARE UNDER PENALTY OF PERJURY THAT THE FOREGOING IS TRUE AND CORRECT.

Executed on June 1, 2007.

By /s/ *Shane Coursen*
Shane Coursen
Senior Technical Consultant
Kaspersky Lab, Inc.

03267/00501 677938.1

Davis Wright Tremaine LLP
LAW OFFICES
2600 Century Square · 1501 Fourth Avenue
Seattle, Washington 98101-1688
(206) 622-3150 · Fax: (206) 628-7699

CERTIFICATE OF SERVICE

I certify that on June 4, 2007, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to the following counsel of record:

Attorneys for Plaintiff
Jeffrey I. Tilden, WSBA No. 12219
Michael Rosenberger, WSBA No. 17730
Gordon Tilden Thomas & Cordell LLP
1001 Fourth Avenue
Suite 4000
Seattle, WA 98154-1051

In addition, paper copies of the foregoing document will be mailed by United States Postal Service to non CM/ECF participants, if any.

/s/ *Bruce E.H. Johnson*
Bruce E.H. Johnson, WSBA No. 7667
Davis Wright Tremaine LLP
2600 Century Square
1501 Fourth Avenue
Seattle, WA 98101-1688
Telephone: (206) 628-7683
Fax: (206) 628-7699
E-mail: brucejohnson@dwt.com

Davis Wright Tremaine LLP
LAW OFFICES
2600 Century Square · 1501 Fourth Avenue
Seattle, Washington 98101-1688
(206) 622-3150 · Fax: (206) 628-7699